INISIATIF SIBER DALAM KONTEKS KEAMANAN SIBER DI FILIPINA

CYBER INITIATIVE IN THE CONTEXT OF CYBER SECURITY IN THE PHILIPPINES

Irwan Septoedy Simbolon[1]

Abstrak - Pokok pada paper ini adalah mengenai strategi keamanan siber yang dilakukan oleh pemerintah Filipina dalam menanggulangi berbagai isu yang dianggap mengganggu ketahanan nasional. Dengan kondisi masyarakat dan pemerintahan yang tidak jauh berbeda, maka kondisi Indonesia sama halnya dengan Filipina dalam hal mengembangkan strategi dan kebijakan yang harus dilakukan untuk mengatasi berbagai ancaman siber. Akan tetapi, Filipina telah melakukan upaya pembentukan institusi-institusi dengan kebijakan yang mengatur peran masing-masing institusi tersebut untuk menghadapi berbagai ancaman siber. Selain itu, pemerintah Filipina juga telah mengimplementasikan *cyber initiative* dengan mengampanyekan *cyber wellness* dan *National Broadband Plan* sebagai program khusus dalam meningkatkan sistem keamanan siber. Dalam menentukan skala prioritas ini, Indonesia dapat mengambil pelajaran tentang bagaimana menentukan strategi dan kebijakan yang tepat untuk menghadapi berbagai ancaman siber yang datang.
Kata kunci: *cybersecurity,* keamanan siber Filipina, ancaman siber, *cyber initiative*

Abstract *- Highlights of this paper is on the cyber security strategy undertaken by the Philippine government in tackling the various issues that were disturbing national security. With the condition of society and a government that is not much different, then the condition of Indonesia as well as the Philippines in terms of developing strategies and policies are needed to address various cyber threats. However, the Philippines has made efforts to establish institutions with a policy governing the role of each of these institutions to confront cyber threats. In addition, the Philippine government has also implemented cyber cyber wellness initiative by campaigning and the National Broadband Plan as a special program in improving cyber security systems. In determining the priorities of this, Indonesia can take lessons on how to determine the appropriate strategies and policies to deal with cyber threats coming.*
Keywords*: cyber security, Philippines cyber security, cyber threat, cyber initiative*

[1] Penulis adalah mahasiswi pasca sarjana Program Studi Peperangan Asimetris Cohort-4 TA. 2016 Fakultas Strategi Pertahanan Universitas Pertahanan. Penulis dapat dihubungi melalui *email* penulis.

Latar Belakang

Pertimbangan tentang pendirian pengadilan khusus dalam menangani kejahatan siber tengah dipertimbangkan oleh Departemen Kehakiman Filipina. Hal ini disebabkan oleh laporan kejahatan siber pada tahun 2014-2015 yang relatif tinggi sehingga pihak Departemen Kehakiman berusaha untuk mengajukan permohonan kepada Mahkamah Agung untuk membentuk pengadilan khusus kejahatan siber yang secara khusus akan menangani segala perkara yang berhubungan dengan siber.

Pada laporan Bulan Maret 2016 yang dirilis oleh gulfnews.com, dikatakan bahwa pembentukan pengadilan khusus tersebut dianggap sesuai dengan aturan hukum, yaitu Pasal 21 Undang-undang Republik Filipina No. 10175 yang di dalamnya terdapat petunjuk tentang perlunya dibuat pengadilan khusus terkait penanganan kejahatan siber yang ditangani oleh hakim khusus, yang sudah terbiasa dalam menangani kejahatan siber. Hingga saat ini, pengadilan yang memiliki kapabilitas dalam menangani kejahatan siber di Filipina masih terbilang sangat sedikit. Meskipun begitu, respon atas tindak kejahatan yang dilakukan oleh masyarakat Filipina di internet terbilang tinggi, termasuk kejahatan pengintaian dengan menggunakan media siber, pencurian hak kekayaan intelektual, seks siber, dan ancaman siber lainnya. Berdasarkan kejahatan-kejahatan siber tersebut, pengintaian dan pencurian hak kekayaan intelektual dianggap sebagai ancaman paling berbahaya bagi pemerintah dan masyarakat Filipina.

Dalam laporan tersebut, disebutkan bahwa serangan pengintaian melalui siber dan pencurian hak kekayaan intelektual merupakan ancaman penting yang secara signifikan telah menyerang berbagai sektor manufaktur serta unit usaha kecil. Meskipun terjadi penurunan kasus dari tahun 2011 ke tahun 2012, tercatat bahwa sebesar 31% target serangan merupakan unit usaha kecil dan konsumen yang dapat diserang dengan menggunakan ancaman *mobile,* terutama android. Unit usaha kecil sendiri menjadi target kejahatan siber akibat terbatasnya keuangan sehingga sulit untuk mengalokasikan dana bagi keamanan siber seperti halnya antiworm, antivirus, dan firewall. Akan tetapi, pihak Kementerian Dalam Negeri Filipina mengklaim bahwa pencapaian terkait keamanan siber sudah dirasa cukup meningkat, terutama dalam hal pembobolan data.

Berdasarkan *Symantec Internet Security Threat Report*, Filipina telah berada pada peringkat ke-35 di tahun 2012 yang secara global telah aktif menangkal ancaman siber. Namun, tren pertumbuhan berbagai ancaman siber tetap perlu diwaspadai oleh organisasi dan lembaga terkait di Filipina, baik pemerintah maupun swasta. Hal ini disebabkan oleh adanya ancaman terstruktur yang bisa saja menimbulkan serangan target tingkat tinggi, ancaman *mobile,* malware, dan pembobolan data yang bisa melumpuhkan seluruh sistem infrastruktur penting di Filipina.

Berdasarkan laporan tersebut, disebutkan bahwa terjadi peningkatan jumlah serangan setiap harinya mulai dari 7 serangan per hari hingga 82 serangan per harinya di tahun 2011. Serangan-serangan tersebut biasanya dilakukan dengan menggunakan teknik *social engineering* dan malware yang sudah dikostumisasi agar dapat memperoleh akses dalam mendapatkan informasi penting. Kasus pembobolan data sendiri merupakan hal yang paling sering terjadi, termasuk terjadinya kasus kehilangan perangkat komputer, media penyimpanan data seperti *smartphone,* USB, dan peralatan data *backup.* Berdasarkan data Kepolisian Nasional Filipina, terutama bidang anti kejahatan siber, tercatat ada 614 kasus kejahatan siber yang dihitung mulai periode Januari hingga Desember 2014. Sebelumnya, kasus kejahatan siber yang terjadi pada tahun 2013 hanya berjumlah 288. Artinya, tindakan kejahatan siber di Filipina dikatakan meningkat sehingga perlu dilakukan upaya yang lebih komprehensif dalam menangani masalah ancaman siber.[2]

Sementara itu, menurut siaran pers dari Kepolisian Nasional Filipina *Anti-Cybercrime Group* (PNP ACG), terdapat 1.211 jumlah total pengaduan kejahatan siber yang diajukan dengan rentang waktu tahun 2013-2015. Lima keluhan teratas yang diterima adalah penipuan online (366), pencemaran nama baik secara online (240), ancaman online (129), pencurian identitas (127), dan foto atau video yang tidak senonoh (89). Sementara itu, jumlah pengguna internet di Filipina yang tercatat sebanyak 44 juta pengguna (tahun 2014). Para pengguna internet ini biasanya menghabiskan rata-rata 18,6 jam per minggu (sekitar 2,6 jam per hari) secara online. PNP ACG juga merilis daftar larangan bagi para

[2] Wijayanto, Doni. (2015). http://yuridis.com/rencana-pembentukan-pengadilan-khusus-kejahatan-siber-di-filipina/

pengguna internet agar tidak menjadi korban kejahatan siber.[3]

Permasalahan ini menjadi penting untuk dikaji karena tingkat kejahatan siber di Filipina tidak jauh berbeda dengan di Indonesia. Diperlukan kebijakan dan strategi yang mampu menghambat dan bahkan memberantas kejahatan siber, baik secara fisik maupun secara psikologis. Di Indonesia, langkah-langkah yang dilakukan juga tidak jauh berbeda dengan di Filipina, yakni mengampanyekan penggunaan internet yang aman bagi seluruh masyarakatnya agar tidak menjadi korban tindak kejahatan siber.

Dengan mendorong setiap masyarakat untuk memahami pentingnya keamanan siber secara menyeluruh, maka pemerintah dapat menerima laporan tentang kondisi keamanan siber sehingga dapat dilakukan upaya pendeteksian secara cepat dan tanggap dalam hal ini. Selain itu, penentuan kebijakan dan strategi tersebut juga perlu mempertimbangkan tren dalam pembentukan keamanan siber, meliputi tren *cyber initiative* yang telah diupayakan oleh berbagai negara. Di Indonesia, *cyber initiative* telah dilakukan sejak tahun 199 dengan adanya Rancangan Undang-undang tentang kebijakan siber. Kebijakan tersebut diatur dalam Rancangan Undang-undang Informasi dan Transaksi Elektronik (ITE) yang meliputi kejahatan siber, transaksi elektronik yang gagal, *digital signature* yang berkembang menjadi kejahata siber, penyalahgunaan komputer, pembocoran *password,* pemanfaatan internet yang salah, hingga permasalahan hak kekayaan intelektual.[4]

Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) pada tahun 2014 mencatat bahwa terdapat 48,8 juta serangan *cyber* di Indonesia akibat adanya aktivitas malware sebanyak 12.007.808 insiden yang meliputi 24.168 kasus kebocoran keamanan, kebocoran rekam jejak atau *record leakage* sebanyak 5.970 kasus, serangan melalui *password harvesting* sebanyak 1.730 kasus, dan serangan akibat kebocoran domain sebanyak 215 kasus.[5]

Akan tetapi, penentuan kebijakan mengenai ITE tersebut juga masih belum diimplementasikan sehingga kemungkinan terjadinya serangan siber

[3] Scitech. (2015). http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes-complaints-in-the-philippines-according-to-pnp

[4] https://id.wikipedia.org/wiki/Hukum_siber

[5] Kompas.com

masih saja bisa meningkat. Selain itu, penggunaan internet di Indonesia juga masih terbilang belum merata karena masih banyak yang belum bisa menggunakan perangkat internet dengan benar sehingga hukum siber di Indonesia masih belum bisa dilakukan. Oleh sebab itu, Indonesia menetapkan langkah-langkah strategis untuk menentukan kebijakan dan keamanan siber dengan berkiblat pada konsistensi *National Security for Homeland Security* yang menjadi pedoman AS dalam mengatasi berbagai macam ancaman siber terhadap infrastruktur yang ada serta melakukan pemulihan atas kerusakan yang diakibatkan oleh serangan siber.[6]

Meskipun Filipina dan Indonesia memiliki kesamaan kondisi masyarakat, namun data kasus kejahatan siber antara Filipina dengan Indonesia terlihat cukup jauh. Oleh sebab itu, diperlukan kajian lebih mendalam mengenai bagaimana *cyber initiative* yang dilakukan oleh negara Filipina sebagai bahan pertimbangan bagi Indonesia dalam menentukan strategi dan kebijakan di ranah siber.

Ancaman Siber dalam *Cyberspace*

Cyberspace adalah hal kontras yang di dalamnya terdapat ruang tidak kasat mata sehingga karena sifatnya yang kontras dianggap sebagai hal yang perlu diapresiasi sebagai hasil karya cipta manusia dengan mempertimbangkan kemungkinan-kemungkinan yang muncul. Hal ini memperlihatkan bahwa *cyberspace* merupakan media virtual dengan tiga lapisan fisik, sintaksis, dan semantik. Lapisan fisik sendiri merupakan bagian pertama yang membentuk dunia siber, yaitu meliputi perangkat komputer dan perangkat keras lainnya. Lapisan sintaksis merupakan sistem *input* dan *output* informasi melalui cara-cara seperti penggunaan mesin, *routing,* format dokumen, manipulasi data, dan lain-lain. Lapisan semantik adalah inti dari sistem kekuatan siber yang di dalamnya semua data akan disimpan sebagai sistem informasi untuk melakukan operasi. Sistem informasi inilah yang menjadi target dari ancaman siber.[7]

Ketiga lapisan tersebut merupakan ancaman bagi setiap negara yang menjalankan sistem infrastruktur melalui *cyberspace.* Misalnya saja, Amerika Serikat yang telah melakukan berbagai operasi menggunakan media siber menganggap

[6] *The National Strategy to Secure Cyberspace.* (2003)

[7] Libicki, 2009, hlm.11-12

bahwa ancaman siber terhadap sistem informasi merupakan prioritas dalam sistem keamanan di negara tersebut. Hal ini juga membuktikan bahwa sistem keamanan AS bergantung pada media siber.

Namun, serangan siber tidak hanya sebatas serangan fisik terhadap sistem infrastruktur saja, tapi juga memiliki pengaruh yang sangat besar terhadap psikologi masyarakat. Misalnya saja, ancaman psikologis yang ditimbulkan akibat foto dan video pornografi yang di hampir semua negara merupakan bagian dari ancaman penting dalam sistem keamanan siber. Oleh sebab itu, diperlukan upaya untuk mengatasi ancaman siber baik secara fisik maupun secara psikologis.

Hukum Siber di Filipina

Berdasarkan Republic Act of The Philippines No. 10175, disebutkan bahwa terdapat upaya Pencegahan Kejahatan Siber yang terdiri atas deklarasi kebijakan yang isinya menyebutkan bahwa negara mengakui peran penting informasi dan industri komunikasi seperti halnya produksi konten, telekomunikasi, penyiaran perdagangan elektronik, dan pengolahan data yang berimplikasi pada pembangunan sosial dan ekonomi bangsa secara menyeluruh. Negara juga mengakui pentingnya penyediaan fasilitas lingkungan yang kondusif dalam hal pengembangan, percepatan, dan aplikasi rasional serta eksplorasi teknologi dan komunikasi untuk memperoleh akses yang gratis, mudah, dan dapat dimengerti demi tujuan penyampaian informasi. Selain itu, terdapat pula kebutuhan untuk melindungi dan menjaga integritas berbagai perangkat siber, sistem komunikasi, jaringan, data, dan ketersediaan informasi dari segala bentuk penyalahgunaan, pelecehan, dan akses ilegal dengan dibuatnya hukum perilaku. Dalam kebijakan ini, negara dituntut untuk memiliki kekuatan yang baik dalam melakukan deteksi dini, penyidikan, penuntutan, dan pencegaha serta pemberantasan kejahatan siber dalam ranah domestik maupun internasional.

Preliminary Provisions

Dalam keamanan siber di Filipina, terdapat istilah-istilah berikut yang perlu dipahami untuk mengetahui ancaman yang mungkin hadir dalam ranah siber.

- Akses, yaitu istilah yang mengacu pada instruksi, komunikasi, penyimpanan data, pengambilan data, dan pemanfaatan sumberdaya sistem komputer dan jaringan komunikasi.

- Modifikasi, yaitu istilah yang mengacu pada perubahan bentuk ataupun substansi data komputer atau program.
- Komunikasi, yaitu istilah yang mengacu pada transmisi informasi melalui media ICT, termasuk dalam hal ini suara, video, dan data lainnya.
- Komputer, yaitu istilah yang mengacu pada perangkat elektronik, magnetik, optik, elektrokimia, maupun pengolahan data lainya yang meliputi tiga lapisan mendasar dari *cyberspace.*
- Data komputer, yaitu istilah yang mengacu pada seluruh bentuk fakta, informasi, maupun konsep yang sesuai untuk diproses dalam sistem komputer. Termasuk program yang dapat menyebabkan fungsi sistem komputer, dokumen elektronik, pesan elektronik, maupun data elektronik yang disimpan dalam komputer lokal maupun yang terjaring.
- Program komputer, yaitu istilah yang mengacu pada instruksi yang dieksekusi oleh komputer untuk mencapai hasil yang diharapkan.
- Sistem komputer, yaitu istilah yang mengacu pada setiap perangkat yang saling berhubungan berdasarkan program tertentu.
- Penyalahgunaan hak dan kekayaan intelektual yang mengacu pada berbagai tindakan yang dilakukan tanpa adanya izin dan yang tidak sesuai dengan alasan hukum, perintah pengadilan, pembenaran, dan prinsip-prinsip hukum yang relevan.
- Istilah siber mengacu pada berbagai jaringan komputer dan media elektronik di mana komunikasi secara online berlangsung.
- Infrastruktur kritis, yaitu istilah yang mengacu pada sistem komputer, jaringan fisik maupun virtual, program komputer, data komputer dan data lalu lintas yang sangat penting bagi negara. Hal-hal tersebut dapat memperlihatkan ketidakmampuan atau kerusakan yang berdampak terhadap sistem keamanan nasional, kesehatan, keselamatan publik, dan lain sebagainya.
- Keamanan siber mengacu pada alat, kebijakan, pendekatan, manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi pengguna siber.

- Database, yaitu istilah yang mengacu pada penyajian informasi, pengetahuan, fakta-fakta, konsep, dan instruksi yang dipersiapkan, diproses, dan disimpan secara formal dalam sistem komputer.
- Intersepsi mengacu pada bagaimana data diperdengarkan, direkam, dipantau, dan diawasi sehingga penyadapan elektronik dapat digunakan untuk keperluan keamanan siber pada saat komunikasi sedang berlangsung.
- Penyedia layanan yang mengacu pada setiap badan pemerintahan maupun swasta yang menyediakan layanan untuk berkomunikasi dengan menggunakan sistem komputer dan setiap entitas yang memproses maupun menyimpan data komputer dengan nama layanan komunikasi.
- *Subscriber's information* yang mengacu pada informasi yang terkandungd alam bentuk data yang disediakan oleh penyedia layanan dan berkaitan dengan konten serta lalu lintas data, serta identitas pengguna.

***Punishable Acts* (Tindak Pidana)**

Dalam Undang-undang Republik Filipina[8], terdapat pasal yang menyebutkan tentang tindak pidana yang berkaitan dengan siber. Salah satunya adalah tindak kejahatan siber yang meliputi tindakan-tindakan berikut ini.

- Pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan sistem dan data komputer.
- Pelanggaran dengan mengaskes sebagian maupun seluruh sistem komputer tanpa sepengetahuan pengguna resmi.
- Penyadapan, baik yang dilakukan dengan menggunakan perangkat komputer maupun jaringan komputer lainnya.
- Interferensi data yang mengacu pada perubahan, perusakan, dan penghapusan data komputer, dokumen elektronik, pesan data elektronik, dan termasuk pengenalan atau transmisi virus.
- Penyalahgunaan perangkat komputer dan sistem jaringannya.
- Penggunaan dan penggandaan data secara ilegal, seperti penggunaan kata sandi, kode akses, atau data lainnya baik sebagian maupun seluruhnya.
- Penyalahgunaan domain dan identitas pengguna internet,

[8] Republic Act of The Philippines, no. 10175

seperti memalsukan identitas, kata sandi, dan penyalahgunaan kekayaan intelektual yang ada di dalamnya.

Selanjutnya, hukum siber di Filipina juga membahas tentang pelanggaran terkait komputer seperti pemalsuan perangkat, input, pengubahan, penghapusan data secara ilegal; penggunaan data komputer untuk melakupan penipuan; dan pencurian identitas yang berkaitan dengan komputer seperti penggunaan, penyalahgunaan, transfer, pengubahan dan penghapusan informasi identitas, serta akuisis.

Pelanggaran selanjutnya yang termasuk ke dalam tindak pidana dalam keamanan siber di Filipina adalah terkait konten pelanggaran yang meliputi keterlibatan, pemeliharaan, kontrol, operasi, dan kegiatan lain yang berhubungan dengan *cybersex* dan pornografi yang dilakukan secara sengaja maupun tidak sengaja; tindakan komersial seperti iklan, penjualan, atau penawaran produk yang dilarang secara hukum; tindakan yang berhubungan dengan perilaku memfitnah; dan pelanggaran lainnya yang juga termasuk ke dalam tindak pidana dalam konteks keamanan siber di Filipina adalah keterlibatan dengan kejahatan siber.

Cyber Wellness Philippines

Dalam menghadapi berbagai ancaman dan pelanggaran terkait siber, Filipina menerapkan program *Cyber Wellness* tentang tindakan proaktif dan positif dalam penggunaan internet, media sosial, dan aplikasi *mobile. Cyber Wellness* memang bukan konsep baru dalam sistem keamanan siber. Konsep ini berkaitan tentang tindakan ideal yang harus dilakukan untuk pengguna internet dalam menggunakan media digital dan aplikasi sosial dan melindungi diri sendiri dari penyalahgunaan siber dan tindakan *bullying* di media online. Kampanye *Cyber Wellness* disuarakan sejak tahun 2010 sebagai titik di mana media sosial dan media online lainnya bergerak bersama-sama melakukan aksi kampanye penggunaan internet secara positif.

Salah satu kegiatan yang diselenggarakan dalam program ini adalah seminar dan edukasi penggunaan media online secara aman yang menghadirkan para relawan dan orang tua untuk saling berbagi pengalaman dalam menggunakan media siber. Seperti dilansir dari websafetyforparents.org, program ini membahas tips keamanan web bagi orang tua yang di dalamnya

orang tua didukung untuk mendidik anak-anak dalam bertanggung jawab atas perilaku di media siber. Baik anak-anak maupun orang tua bisa saja menjadi target dari kejahatan siber, terutama *cyber bullying* yang sampai saat ini masih menjadi isu utama. Oleh sebab itu, hukum anti kejahatan siber, anti-bullying, dan privasi data menjadi prioritas dalam sistem keamanan siber di Filipina.

Dalam program ini, pendekatan dilakukan secara holistik dengan melibatkan seluruh pemangku kepentingan sehingga edukasi bagi orang tua, anak-anak, dan akademisi menjadi bagian dari pertahanan terbaik dalam sistem keamanan siber. Tidak hanay itu, beberapa LSM juga dilibatkan untuk memfasilitasi kegiatan edukasi tentang bagaimana mempergunakan siber dengan baik dan positif. Beberapa sekolah di Filipina juga sudah memasukkan program *cyber wellness* untuk pengembangan pendidikan. Dalam program ini, pemangku kepentingan yang dilibatkan meliputi pemerintah, pihak administrasi sekolah, anggota fakultas dan bimbingan konselor, orang tua, siswa, karyawan, dan LSM.

Secara umum, tujuan utama dari program ini adalah untuk 1) menyejajarkan kebijakan edukatif yang sesuai dengan kerangka hukum, pedoman Kementrian Pendidikan; 2) meningkatkan kebijakan perusahaan untuk merepresentasikan ketentuan kejahatan siber dan hukum privasi data; 3) memberikan intervensi pembelajaran yang dapat meningkatan penggunaan internet secara positif dan proaktif; 4) melindungi diri pengguna internet dari pengalaman negatif yang diakibatkan oleh pelanggaran terkait hukum siber yang berlaku; dan 5) mengetahui respon yang harus dilakukan untuk menghadapi permasalahan-permasalahan tersebut.[9]

Dalam menggalakkan program ini, pemerintah dan pihak lain yang terlibat bekerja sama secara terbuka untuk mencapai kepentingan nasional dalam konteks keamanan siber, meskipun masing-masing lembaga memiliki perbedaan inisiatif. Program ini juga menyediakan fasilitas bagi korban *cyber bullying* untuk memberikan pendapatnya mengenai kejahatan siber yang pernah atau sedang menimpa mereka. Masyarakat dapat berpartisipasi dengan membuat program akademik dan non akademik untuk anak-anak sekolah, berkolaborasi dengan Kementrian Pendidikan, dan mengembangkan seminar-seminar untuk memberikan

[9] asksonnie.info/cyber-wellness-philippines/

awareness tentang pentingnya *cyber wellness.*

***Cyber Inisiative* Pemerintah Filipina**

Strategi Filipina dalam menghadapi era digital adalah dengan membentuk *Philippine Cable Television Association* (PCTA) yang bekerja sama dengan *DOST-ICTO* untuk mendukung pembangunan TIK Nasional. Kerjasama ini dibentuk untuk mendukung advokasi fungsi dan pelaksanaan yang efektif dari *Philippine Digital Security* (PDS). Pembentukan DOST-ICTO[10] mendukung pemerintahan Filipina saat ini dengan memulai beberapa program ICT.

Salah satu tujuan utama pembentukan DOST-ICTO ini adalah untuk meningkatkan pelayanan pemerintah kepada masyarakat Filipina dalam hal kecepatan, efisiensi, transparasi, dan akuntabilitas *cyberspace.* Salah satu program yang sudah dikembangkan adalah melalui *e-Government* yang mengintegrasikan layanan pemerintah gratis untuk memastikan kemudahan publik dalam melakukan akses di dunia siber secara terfokus. Tujuannya adalah untuk membangun, meningkatkan, dan memperbaiki infrastruktur, sistem, dan prosedur yang terkait dengan TIK.

Dalam hal ini, DOST-ICTO telah mengidentifikasi sistem prioritas yang akan diintegrasikan seperti halnya sistem perizinan usaha, sistem pajak, dan sistem pembayaran yang bernaung di bawah portal *e-Government.* Dengan demikian, diperlukan penyediaan konektivitas tanpa batas dari tingkat nasional hingga ke tingkat rumah tangga yang di dalamnya dibutuhkan pula dukungan dari PCTA.

Sebagai bagian dari program prioritas, DOST-ICTO akan merumuskan *National Broadband Plan* untuk lima tahun ke depan yang akan memberikan arah yang jelas bagi pemerintah Filipina dalam memastikan bahwa semua masyarakat Filipina akan memperoleh keuntungan dari program tersebut. *National Broadband Plan* ini diharapkan mampu memberikan pencapaian yang baik dalam strategi penyebaran broadband nasional. *National Broadband Plan* ini juga akan digunakan untuk menganalisis perencanaan pemerintah dan sektor swasta dalam hal penggunaan internet sehingga pemerintah memiliki "pintu" yang dapat mengetahui data-data yang masuk dan keluar melalui sistem informasi. Hal ini akan memungkinkan keamanan tambahan untuk data dan transaksi yang dilakukan oleh pemerintah dan masyarakat.

[10] Department of Science and Technology-Information and Communication Technology Office

Selama satu dekade terakhir, negara-negara berkembang telah melihat pertumbuhan dramatis dalam sektor teknologi informasi dan komunikasi (ICT), terutama pada langganan telepon seluler dan penggunaannya. Negara ini memiliki sekitar penetrasi 90% dalam hal penggunaan ponsel. Namun, sebagian besar negara-negara berkembang seperti Filipina, memiliki keterbelakangan dalam hal adopsi dan penggunaan broadband sehingga memungkinkan terjadinya kesenjangan digital yang dapat menghambat pembangunan ekonomi dan inklusi sosial karena sejumlah besar individu masih tidak memiliki akses internet berkecepatan tinggi.

National Broadband Plan juga akan memastikan bahwa serangkaian strategi dan tindakan akan diimplementasikan untuk mencapai seperangkat indikator pada akses internet agar setiap orang dapat memperoleh keuntungan dari penggunaan internet dengan akses yang cepat dan mudah. Beberapa program yang dihimpun oleh *Philippine Digital Strategy* (PDS) dalam rentang waktu 2011-2016 adalah sebagai berikut.

- 80% dari masyarakat memiliki akses internet melalui Cecs minimal 2 Mbps.
- 100% sekolah tinggi & 80% dari sekolah dasar memiliki akses internet.
- 80% dari lembaga publik lainnya memiliki akses internet.
- 100% dari kantor pemerintah memiliki akses internet.
- Semua distrik pusat bisnis memiliki kecepatan *download* yang tersedia dari 20 Mbps.
- 80% rumah tangga memiliki akses konektivitas broadband setidaknya 2 Mbps.
- Harga rata-rata untuk Internet broadband dasar harus dikurangi setidaknya 5% per tahun.
- Investasi dalam ekspansi infrastruktur ditingkatkan setidaknya 10% per tahun.

National Broadband Plan ini pada dasarnya adalah sebuah program yang diselenggarakan oleh pemerintah beserta pemangku kepentingan lainnya agar seluruh lapisan measyarakat dapat mempergunakan internet sebagai media infrastruktur. Hal ini berarti bahwa seluruh lapisan masyarakat akan memperoleh edukasi terkait penggunaan internet secara menyeluruh, hingga

akhirnya dapat melaksanakan program *cyber wellness.*[11]

Implementasi Program *Cybersecurity* di Filipina

Strategi dan kebijakan mengenai keamanan siber nasional di Filipina pertama kalinya diimplementasikan pada tahun 2004 dengan tujuan utama untuk melindungi infrastruktur negara dan perusahaan swasta dari ancaman siber. Meskipun begitu, pemerintah Filipina masih menempatkan kebijakan dan langkah-langkah yang harus ditempuh mengenai penggunaan siber dalam suatu perusahaan berdasarkan kesadaran masing-masing pihak yang terlibat dengan tetap berfokus pada Satuan Tugas Keamanan Infrastruktur Kritis (TFSCI) dan Kelompok Kerja Keamanan Cyber (CySWG). Keduanya telah menentukan sebelas sektor penting yang harus dimasukkan ke dalam program keamanan siber di Filipina dengan mempersiapkan strategi nasional untuk kebutuhan perlindungan infrastruktur kritis.

Sebelas sektor penting yang dimaksud meliputi energi, pasokan air, informasi dan komunikasi, transportasi, perbankan dan keuangan, kesehatan masyarakat, layanan darurat, pertanian dan makanan, manufaktur, layanan pemerintah, dan pusat komersial. Selain itu, implementasi program *cybersecurity* yang efektif juga menerapkan enam prioritas.[12]

Prioritas pertama adalah berusaha mendirikan rezim hukum keamanan siber yang menguntungkan seluruh masyarakat Filipina dan memberlakukan hukum untuk kejahatan siber. Program ini tidak hanya melibatkan aktor nasional saja, tapi juga aktor negara lain sehingga perjanjian bilateral dan multilateral dibentuk untuk memenuhi tujuan keamanan siber nasional di Filipina. Perjanjian internasional ini dibuat untuk kepentingan dukungan, baik berupa sokongan dana untuk memenuhi kinerja program keamanan siber nasional Filipina, maupun untuk keperluan penasihat.

Prioritas kedua adalah dengan mengurangi kerentanan infrastruktur kritis dalam konteks keamanan siber nasional. Dalam prioritas yang satu ini, diperlukan rencana risiko dan penilaian kerentanan untuk mengidentifikasi daerah-daerah mana saja yang rentan

[11] http://icto.dost.gov.ph/philippine-governments-ict-initiatives-and-the-national-broadband-plan/ diakses 24 Juli 2016

[12] http://www.itworldcanada.com/article/philippines-to-implement-cybersecurity-program/16895

terkena ancaman siber. Pemerintah juga perlu melakukan pengawasan yang ketat terhadap anacaman dan risiko dari berbagai program yang dijalankan.

Prioritas selanjutnya adalah program kampanye kesadaran bagi perusahaan, baik pemerintah maupun swasta. Sektor swasta akan didorong untuk memberikan dukungan dalam program sertifikasi keamanan siber profesional yang terkoordinasi dan membantu melatih korps ilmuwan komputer muda yang akan memiliki keahlian di bidang siber. Prioritas ini akan terkoordinasi pada tim pusat yang menaungi tingkat nasional, regional dan sektoral. Pelaksanaan Alert Nasional dan Sistem Peringatan serta pembentukan program bantuan untuk keadaan darurat dalam konteks keamanan siber juga dipertimbangkan dalam prioritas ini. Oleh sebab itu, pemerintah juga memberikan sejumlah program pelatihan keamanan, termasuk pelatihan khusus investigasi teknis dan perang informasi yang akan diberikan anggaran khusus.

Prioritas keempat adalah dengan mengadakan penelitian yang berkaitan dengan sistem keamanan siber. Pemerintah mempertimbangkan pemberian kredit pajak dan meningkatkan kemampuan pembangunan serta penelitian di dalam konteks keamanan siber dengan dibentuknya DOST.

Prioritas kelima adalah dengan melibatkan pembentukan mekanisme terkoordinasi secara nasional dan internasional yang mencakup *cyber intelligence* untuk kebutuhan pendeteksian adanya ancaman siber.

Kesimpulan

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa pemerintah Filipina telah melihat ancaman siber sebagai salah satu ancaman yang dapat melumpuhkan infrastruktur kritis sehingga dibentuklah lembaga-lembaga yang secara terkoordinasi mampu melaksanakan perannya dalam konteks keamanan siber.

Cyber initiative dalam konteks keamanan siber di Filipina merujuk pada penggunaan internet di dalam ruang lingkup masyarakat nasional yang merata sehingga tidak terjadi ketimpangan digital yang mengakibatkan kurangnya pengetahuan masyarakat terhadap ancaman siber.

Kondisi inilah yang memunculkan program *National Broadband Plan* serta program *Cyber Wellness* dengan tujuan utama memberikan akses yang mudah kepada masyarakat dalam mendapatkan pelayanan publik serta memberikan

pengetahuan akan pentingnya kesadaran berperilaku positif pada saat mempergunakan internet.

Filipina sendiri telah menentukan skala prioritas yang harus dimiliki dan ditindaklanjuti untuk memenuhi tujuan utama tersebut sehingga langkah-langkah, strategi dan kebijakan yang dibutuhkan pun akan diimplementasikan berdasarkan skala prioritas tersebut.

Sementara itu, Indonesia merupakan negara yang dapat dikatakan lebih maju daripada Filipina. Rencana dibentuknya Badan Cyber Nasional (BCN) yang segera berdasarkan keputusan presiden akan diarahkan untuk menjadi koordinator bagi upaya perlindungan keamanan siber di Indonesia. Badan Cyber Nasional inilah yang akan menyiapkan rencana undang-undang cyber untuk kemudian diaplikasikan demi keamanan siber nasional di Indonesia. BCN ini akan diarahkan sebagai koordinator yang sinergis dalam melakukan koordinasi, sinkronisasi, dan eksekusi segala macam permasalahan di *cyberspace* tanpa melangkahi kewenangan institusi terkait lainnya.

Akan tetapi, terdapat kendala teknis yang menghambat pembentukan BCN hingga saat ini. Salah satunya adalah banyaknya institusi yang merasa memiliki kewenangan untuk menjadi *leading sector* dalam hal ini. Hal ini disebabkan oleh adanya beberapa institusi yang memiliki peran utama dalam konteks keamanan siber seperti *Cyber Defence* yang merupakan wilayah kewenangan dari Kementerian Pertahanan dan TNI; *Cyber Crime* yang merupakan wilayah kewenangan Polri dan Kejaksaan dengan peran menjaga ketertiban masyarakat dan ketertiban umum; *Cyber Inteligence* yang merupakan wilayah kewenangan BIN dan Lembaga Sandi Negara dengan peran deteksi dan peringatan dini, serta pengamanan informasi; *Cyber Security* yang merupakan kewenangan Kemkominfo dan Kemdagri dalam perannya sebagai pelayanan publik dan administrasi penduduk; *Cyber Resilience* yang merupakan kewenangan Kemenko Polhukam dan Dewan Ketahanan Nasional yang berfungsi untuk melakukan koordinasi, sinkronisasi, pengendalian, dan ketahanan nasional; serta *Cyber Diplomacy* yang merupakan kewenangan Kemenlu dengan fungsi diplomasinya.[13]

Selain itu, Filipina juga memiliki keunggulan dalam menentukan skala prioritas yang harus dilakukan untuk

[13] Soepardi, Hanni Sofia, http://www.antaranews.com/berita/565176/bcn-diarahkan-jadi-koordinator-keamanan-siber-indonesia

menangani ancaman siber. Sementara di Indonesia, belum ada rancangan program yang secara khusus melakukan pendeteksian terhadap aspek apa saja yang sangat krusial untuk diprioritaskan terkait isu ancaman siber yang mungkin terjadi.

Daftar Pustaka

ASKSonnie, '*Cyber Wellness Philippines'*, (online), http://asksonnie.info/cyber-wellness-philippines/ diakses 23 Juli 2016.

Kajian Pembentukan Badan Cyber Nasional Sudah Selesai, 2015, (online) http://nasional.kompas.com/read/2015/09/26/03060021/Kajian.Pembentukan.Badan.Cyber.Nasional.Sudah.Selesai diakses 21 Juli 2016.

Libicki, Martin C, '*Cyberdeterrence and Cyberwar'*, RAND Project Air Force, 2009.

Scitech, '*Top 5 Cybercrime Complaints in The Philippines, According to PNP'*, 27 Agutus 2015, (online), http://www.gmanetwork.com/news/story/534597/scitech/technology/top-5-cybercrimes-complaints-in-the-philippines-according-to-pnp diakses 20 Juli 2016.

Philippine Government's ICT Initiatives and the National Broadband Plan, 2016, (online), *http://icto.dost.gov.ph/philippine-governments-ict-initiatives-and-the-national-broadband-plan/* diakses 23 Juli 2016.

Ramos, Geoffrey P, '*Philippines to Implement Cybersecurity Program'*, 9 Agustus 2004, (online), http://www.itworldcanada.com/article/philippines-to-implement-cybersecurity-program/16895 diakses 23 Juli 2016.

Republic Act of The Philippines, (online), http://www.gov.ph/2012/09/12/republic-act-no-10175/ diakses 21 Juli 2016.

Soepardi, Hanni Sofia, '*BCN Diarahkan jadi Koordinator Kemanan Siber Indonesia'*, 4 Juni 2016, (online), http://www.antaranews.com/berita/565176/bcn-diarahkan-jadi-koordinator-keamanan-siber-indonesia, diakses 23 Juli 2016.

The National Strategy to Secure Cyberspace, The White House Washington, 2003.

Wijayanto, Doni, '*Rencana Pembentukan Pengadilan Khusus Kejahatan Siber di Filipina'*, 9 April 2015, (online), http://yuridis.com/rencana-pembentukan-pengadilan-khusus-kejahatan-siber-di-filipina/ diakses 20 Juli 2016.

https://id.wikipedia.org/wiki/Hukum_siber diakses pada 20 Juli 2016.